PANEL: INFORMATION ASSURANCE FOR UK GOVERNMENT

PANEL POSITION PAPERS

Chairman: John Doody CESG

RESUME FOR PANEL INFORMATION ASSURANCE FOR UK GOVERNMENT

By

John Doody

In 1997 the UK Government launched a programme called “Modernising Government”, the aim was to have government departments connected electronically and also to provide a communications and security architecture that would eventually allow the UK citizen to access government departments.

Part of the Modernising Government initiative was the launch of the Government Secure Intranet (GSI), this network currently consists of 140,000 terminals connected in LANs which are in turn connected to the GSI and information classified RESTRICTED can be passed securely between government departments. The GSI is also connected to the Internet via Firewalls, users of the GSI thus have an additional benefit of communicating through the Internet to other agencies at the UNCLASSIFIED level.

The target set for the development of the GSI is 25% of government departments to be connected to the GSI and conducting business electronically by 2001 and 100% including citizen access by 2005.

The challenge facing the security authorities was how to implement a secure architecture that would allow the safe handling of both classified and unclassified information. The UK series of presentations will highlight the development of the GSI, case studies associated with the rules in place to join the GSI and the impact and relevance of BS7799
In setting security standards.

The UK panel consists of subject matter experts from the UK National Security Authority, CESG, the UK Ministry of Defence and two other major government departments.

Panel Co-ordinator and Speaker 1: Dr Roger Griffin CMPS

CONNECTING THE CIVIL SERVICE COLLEGE TO THE GOVERNMENT SECURE INTRANET

By

Dr Roger Griffin

The Civil Service College.

Previously an extremely successful Cabinet Office "Next Steps" Agency, the College was integrated into the Centre for Management and Policy Studies on 1st April 2000.
CMPS has a training element of some 300 persons covering a range of topics such as training for the UK and European fast stream civil servants, management training and training for specialists requiring human resources, project management and other professional qualifications. Considerable resources are deployed in the provision of training and consultancy for Overseas Governments.

Information System.

Based on 5 servers running specialist in house applications and Microsoft Office applications running over Windows NT 4.0 with service pack 4. The system is connected via ISDN links to College Offices in Glasgow and Edinburgh and caters for a total user population of approximately 300 persons.

Staff Culture.

The College has its own permanent staff members, academics, specialists and senior civil servants and also works with a large number of public and private sector associates. The GSI can transmit information protectively marked at Restricted between its departmental users and organisations wishing to connect must be able to demonstrate a security culture amongst their staff and their ability to safeguard HMG information.

Accreditation Issues.

The accreditation process requires a formal risk analysis of the system and its environment, the production of the relevant documentation (system security policy and security operating

Conclusion.

Work commenced early in 1998, on the College system accreditation process. Formal application to connect was made to the GSI Accreditation Panel in April 2000 and the College received GSI accreditation on 11 May 2000.

Speaker 2: Terry Wells DETR

BS7799 THE BRITISH STANDARD FOR INFORMATION SECURITY MANAGEMENT APPLICATION WITHIN DETR

By

Terry Wells

BS 7799 is the British Standard for Information Security Management, and is concerned with protecting an organisation's information processes so that the organisation may get on with its business without disruption.

Developed from a voluntary code of practice created by a group of private sector companies, the standard has gained widespread acceptance both in the UK and around the World, and is now on its way to becoming an ISO standard.

The standard includes best practice advice and a specification for an Information Security Management System, and provides the basis for a formal certification scheme. In addition to enabling organisations to achieve an auditable standard of information security, it can assist in establishing a trust relationship between organisations that wish to do business in a secure manner.

The UK Government has recognised that the standard, applied in combination with internal government security regulations, is appropriate for use within government. The experience of the UK's Department of the Environment, Transport, and the Regions in preparing to achieve compliance with the standard in the information security management of its key information processes is used as an example.

The presentation is of interest to those who wish to hear about: a British Standard that is on its way to becoming an ISO standard; the application of a private sector standard in a government

Speaker 3: John Laskey Home Office

UK HOME OFFICE – FROM GOVERNMENT SECURE INTRANET (GSI) TO BS 7799

By

John Laskey

What my office does.

The Home Office *Departmental Security Unit* (DSU) is responsible for overall security in the Home Office, including advice, guidance and training. Infosec is the youngest discipline in the Unit. Some security responsibilities have been devolved to sub-organisational units.

What the Home Office does/why it needed GSI.

A major UK department of state with its origins dating back to the Revolutionary War period, the Home Office now roughly equates to the US Department of Justice. The UK government is committed to modernising its infrastructure and aims to adapt the most modern IT solutions to all of its business. Home Office business managers quickly recognised the significance of getting on the GSI as an essential part of its plans to use both Internet and Intranet facilities.

How DSU helped.

It is a condition of GSI connection that applicants must first have formally accredited their network to RESTRICTED (i.e. roughly equating to the U.S. 'sensitive but unclassified' marking) level of operation. DSU's task was to convince the GSI Accreditation Panel, comprising the UK Security Authorities, that allowing the new Home Office network to join would not pose unacceptable security risks to the GSI, or to any networks already connected to it. The DSU championed security issues within the network building and GSI application projects, supporting IT managers not familiar with Infosec to ensure that central government security rules and advice were built into both.

Impact and aftermath.

The GSI has enabled a change to the working culture of our 218 year-old department, and most headquarters staff enjoy instant access to research information on the web, including all the

Why the Home Office needs BS 7799 accreditation.

Getting GSI accreditation was an important milestone in establishing a standard approach to Infosec throughout the Home Office. Around this time, another important IT planning benchmark had been established through departmental initiatives to manage Y2K contingency plans. Against this background, UK central government had been encouraging all departments of state to adopt the BS7799 security standard, and to formally report back on progress by December 2000. DSU welcome the standard's recognition of the need for a holistic approach to security. We believe that it formalises good practice, and ought not to require radical reengineering of established security processes.

Conclusion.

The Home Office has not always been at ease with new technologies or business practices. There is still much progress to be made in its modernisation programme, but the implementation of government lead Infosec initiatives, such as GSI and BS7799, continue to play a major role in its forward progress.

Speaker 4: John Peters MOD

SHARED ENVIRONMENTS BETWEEN
THE MINISTRY OF DEFENCE AND ITS PARTNERS

By

John Peters

Shared Data Environments

The Ministry of Defence's Smart Procurement initiative aims to shorten the timescale from contract placement to in-service date for Defence programmes. Integrated Project Teams formed from the stakeholders in a project will manage projects. The stakeholders include the user, logistic, scientific, procurement and related industry communities.

The Joint Enterprise Integration Task Force was tasked with accelerating the sharing of information across the defence sector in support of Smart Procurement. Security was perceived as the major inhibitor, therefore priority was given to assessing the issues and to identifying solutions for the implementation of secure Shared Data Environments (SDEs).

Defence E-Commerce Service

E-commerce services are different from SDEs, being a series of short-term transaction processes for the supply of goods and services including electronic catalogues, order management and tracking capabilities.

The Defence Logistics Organisation is overhauling the provision of its support in order to reduce operating costs and increase operational effectiveness over the next 4 years. A main initiative is the Defence E-Commerce Service (DECS) project, which will provide bridge between existing systems and the suppliers of goods and services. DECS will support new business processes for procurement. DECS will utilise e-mail and Web browsing.

International Collaborations

The 5 nation Defence IT Security Working Group has produced a Common Accreditation Process for collaborative exercises and programmes involving shared information systems. The MOD has established procedures for the evaluation, certification and accreditation of multi-national systems.

Accreditation Issues

The shared environments and their connection to the systems of disparate partners, possibly applying different security regimes, requires a mixture mutual recognition of accreditation and the application of common generic standards.